Kolyvagin's Conjecture and Higher Congruences of Modular Forms

Naomi Sweeting

(Harvard)

January 19, 2023
Banff

Introduction

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.

Introduction

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.
- Idea: use $X_0(N) \to E$ to produce rational points.
- If $K/\mathbb{Q}$ is an imaginary quadratic field in which all $\ell | N$ are split, then $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{N}^{-1}$ is a $K[1]$-rational point $y(1)$ of $X_0(N)$.
- If $(n, N) = 1$, then have $y(n) \in X_0(N)(K[n])$ CM point of conductor n.

Gross-Zagier

Let $y_K \in E(K)$ be the trace of image of $y(1)$.

Theorem (Gross-Zagier)

$L'(E/K,1) \neq 0 \iff y_K \in E(K)$ is non-torsion.
In particular, $r_{an} = 1 \implies r_{MW} \geq 1$.

- Note $L(E/K,s)$ vanishes to odd order at $s = 1$ by splitting conditions.

Kolyvagin's classes

- Fix auxiliary p with $E[p]$ absolutely irreducible, and image of Galois action on $E[p]$ containing a nontrivial scalar.

- For $n = \prod \ell$ with ℓ inert in K, Kolyvagin defined classes

$$c(n) \in H^1(K, T_pE/I_n)$$

  using CM points $y(n)$.

  - $I_n = (a_\ell, \ell + 1) \subset \mathbb{Z}_p$.

Kolyvagin's classes

- Fix auxiliary p with $E[p]$ absolutely irreducible, and image of Galois action on $E[p]$ containing a nontrivial scalar.

- For $n = \prod \ell$ with ℓ inert in K, Kolyvagin defined classes

$$c(n) \in H^1(K, T_pE/I_n)$$

  using CM points $y(n)$.

  - $I_n = (a_\ell, \ell + 1) \subset \mathbb{Z}_p$.
  - When $n = 1$,

$$c(1) = \delta(y_K) \in H^1(K, T_pE)$$

    where $\delta =$ Kummer map.

Kolyvagin's classes

- Fix auxiliary p with $E[p]$ absolutely irreducible, and image of Galois action on $E[p]$ containing a nontrivial scalar.

- For $n = \prod \ell$ with ℓ inert in K, Kolyvagin defined classes

$$c(n) \in H^1(K, T_pE/I_n)$$

  using CM points $y(n)$.

  - $I_n = (a_\ell, \ell + 1) \subset \mathbb{Z}_p$.
  - When $n = 1$,

$$c(1) = \delta(y_K) \in H^1(K, T_pE)$$

    where $\delta =$ Kummer map.

  - $c_M(n) \in H^1(K, E[p^M]) =$ reduction of $c(n)$ when $M \leq v_p(I_n)$

Kolyvagin's conjecture

Let $\nu \leq \infty$ be the least integer s.t. $\exists n$ with ν prime factors and with $c(n) \neq 0$.

Conjecture (Kolyvagin)

There exists n such that $c(n) \neq 0$, i.e. $\nu < \infty$.

Kolyvagin's conjecture

Let $\nu \leq \infty$ be the least integer s.t. $\exists n$ with ν prime factors and with $c(n) \neq 0$.

Conjecture (Kolyvagin)

There exists n such that $c(n) \neq 0$, i.e. $\nu < \infty$.

Let $r_p^{\pm} = rank_{\mathbb{Z}_p} \mathrm{Sel}(K, T_p E)^{\pm}$, where $\pm$ denotes τ eigenvalue.

Theorem (Kolyvagin)

Suppose $\nu < \infty$. Then $\max\left\{r_p^+, r_p^-\right\} = \nu + 1$, $\min\left\{r_p^+, r_p^-\right\} \leq \nu$, and total rank is odd.

Gross-Zagier and Kolyvagin

Theorem (Gross-Zagier)

$L'(E/K,1) \neq 0 \iff y_K \in E(K)$ is non-torsion.

Theorem (Kolyvagin)

If y_K is non-torsion, then $r_{MW} = r_p^+ + r_p^- = 1$.

- y_K non-torsion $\iff c(1) \neq 0 \iff \nu = 0$.
- Then $r_p^+ + r_p^- \leq 2\nu + 1 = 1$.

Converse to GZK

Proposition 1

Suppose $\nu < \infty$ *and* $r_p^+ + r_p^- = 1$*. Then* $L'(E/K, 1) \neq 0$*. In particular,* $r_{an} = r_{MW} = 1$ *and* Ш_p *is finite.*

- Since $\nu < \infty$, have $r_p^+ + r_p^- \geq \nu + 1$ so $\nu = 0$
- Therefore $c(1) \neq 0$, and y_K is non-torsion.

Generalized set-up

- Fix K an imaginary quadratic field, $N = N^+ N^-$ with all $\ell | N^+$ split and all $\ell | N^-$ inert, N^- squarefree with $\nu(N^-)$ even.
- X_{N^+,N^-} = Shimura curve associated to quaternion algebra B of discriminant N^- and $\Gamma_0(N^+)$ level structure.
- Can define CM points $y(n) \in X_{N^+,N^-}(K[n])$, coming from $K \hookrightarrow B$. In moduli interpretation, these will be (isogenous to) products of CM elliptic curves, with action of $B \hookrightarrow M_2(K)$
- $\exists$ modular parameterization $J_{N^+,N^-} \to E$

Main result

Theorem (S., 2021)

For such K and N, let $E/\mathbb{Q}$ be a non-CM elliptic curve of conductor N and $p \nmid 2D_K N$ a prime. Assume:

- $\nu(N^-)$ is even.
- $\overline{\rho} : G_{\mathbb{Q}} \to E[p]$ is absolutely irreducible and image contains a nontrivial scalar; if $p = 3$, then $\overline{\rho}$ is not induced from a character of $G_{\mathbb{Q}[\sqrt{-3}]}$.
- If p is inert in K or $p|a_p$, then $\exists\ \ell || N$ of non-split toric reduction.

Then there exists n with $c(n) \neq 0$, i.e. $\nu < \infty$.

- In particular, $r_p^+ + r_p^- = 1 \iff L'(E/K, 1) \neq 0$.

Main result

Theorem (S., 2021)

For such K and N, let $E/\mathbb{Q}$ be a non-CM elliptic curve of conductor N and $p \nmid 2D_K N$ a prime. Assume:

- $\nu(N^-)$ is even.
- $\overline{\rho} : G_{\mathbb{Q}} \to E[p]$ is absolutely irreducible and image contains a nontrivial scalar; if $p = 3$, then $\overline{\rho}$ is not induced from a character of $G_{\mathbb{Q}[\sqrt{-3}]}$.
- If p is inert in K or $p|a_p$, then $\exists\ \ell || N$ of non-split toric reduction.

Then there exists n with $c(n) \neq 0$, i.e. $\nu < \infty$.

- Zhang proved some $c_1(n) \neq 0$ assuming $E[p]$ is ramified at $\ell | N^+ +$ other hypotheses.
- Moral: rank 0 BSD + congruences $\implies$ Kolyvagin.

“Kolyvagin classes” when $\nu(N^-)$ odd

- Let X_{N^+,N^-} be the Shimura set associated to quaternion algebra B ramified at $N^-\infty$, and $\Gamma_0(N^+)$ level structure.

$$X_{N^+,N^-} = B^\times \backslash B(\mathbb{A}_f)^\times / \widehat{R}^\times$$

- If f is the modular form associated to E, then by JL we have

$$\phi_f : X_{N^+,N^-} \to \mathbb{Z}$$

with the same eigenvalues.

"Kolyvagin classes" when $\nu(N^-)$ odd

- Let X_{N^+,N^-} be the Shimura set associated to quaternion algebra B ramified at $N^-\infty$, and $\Gamma_0(N^+)$ level structure.

$$X_{N^+,N^-} = B^\times \backslash B(\mathbb{A}_f)^\times / \widehat{R}^\times$$

- If f is the modular form associated to E, then by JL we have

$$\phi_f : X_{N^+,N^-} \to \mathbb{Z}$$

with the same eigenvalues.

- If $\ell | N^+$ are split and $\ell | N^-$ are inert in K, then have "CM points" $y(n) \in X_{N^+,N^-}$.

"Kolyvagin classes" when $\nu(N^-)$ odd

- We define $\ell(n) \in \mathbb{Z}_p/I_n$ for Kolyvagin numbers n using $\phi_f(y(n))$.
- Likewise $\ell_M(n) \in \mathbb{Z}_p/p^M$.
- $\ell(1)$ is a unit multiple of $L^{alg}(E/K,1)$ (Gross).
- Let $\nu \leq \infty$ be the smallest integer s.t. $\exists n$ with ν prime factors s.t. $\ell(n) \neq 0$.

A result for $\nu(N^-)$ odd

Theorem (S., 2021)

K, N, p, E as before, but $\nu(N^-)$ is odd. Then:

- $\exists n$ with $\ell(n) \neq 0$, i.e. $\nu < \infty$.
- $\max\left\{r_p^+, r_p^-\right\} = \nu$.
- $r_p^+ + r_p^-$ is even.

- When $r_p^\pm = 0$, this follows from BSD formula (in rank zero), i.e. $L(E/K, 1) \neq 0 \iff rk_{\mathbb{Z}_p} \mathrm{Sel}(K, T_pE) = 0$.

A two-variable Euler system

- Whenever $\nu(N^- Q)$ is even, all $q|Q$ are inert, and

$$T_p J_{N^+,N^-Q} \twoheadrightarrow T_p E/p^M \simeq E[p^M], \qquad \text{(level-raising)}$$

we may define $c_M(n, Q)$ using $y(n, Q) \in J_{N^+,N^-Q}(K[n])$ and induced map

$$H^1(K, T_p J_{N^+,N^-Q}) \to H^1(K, E[p^M]).$$

A two-variable Euler system

- Whenever $\nu(N^- Q)$ is even, all $q|Q$ are inert, and

$$T_p J_{N^+, N^- Q} \twoheadrightarrow T_p E/p^M \simeq E[p^M], \qquad \text{(level-raising)}$$

  we may define $c_M(n, Q)$ using $y(n, Q) \in J_{N^+, N^- Q}(K[n])$ and induced map

$$H^1(K, T_p J_{N^+, N^- Q}) \to H^1(K, E[p^M]).$$

- Whenever $\nu(N^- Q)$ is odd, all $q|Q$ are inert, and

$$\mathbb{Z}[X_{N^+, N^- Q}]^0 \twoheadrightarrow \mathbb{Z}/p^M(f), \qquad \text{(level-raising)}$$

  can define

$$\ell_M(n, Q) \in \mathbb{Z}/p^M$$

  using $y(n, Q) \in X_{N^+, N^- Q}$.

A two-variable Euler system

- Geometric arguments + control on failure of $\mathbb{T}$-freeness for $T_p J_{N^+,N^-Q}$ and $X_{N^+,N^-Q} \implies$ plenty of level-raising congruences.

So we have constructed:

$$\begin{cases} c_M(n,Q) \in H^1(K, E[p^M]), & \nu(N^-Q) \text{ even} \\ \ell_M(n,Q) \in \mathbb{Z}/p^M, & \nu(N^-Q) \text{ odd} \end{cases}$$

for $M \leq v_p(I_n), M(Q)$.

A two-variable Euler system

$$\begin{cases} c_M(n,Q) \in H^1(K, E[p^M]), & \nu(N^- Q) \text{ even} \\ \ell_M(n,Q) \in \mathbb{Z}/p^M, & \nu(N^- Q) \text{ odd} \end{cases}$$

Two-variable Euler system relations:

- Horizontal:

$$\operatorname{ord} \operatorname{loc}_\ell c_M(n,Q) = \operatorname{ord} \operatorname{loc}_\ell c_M(n\ell, Q)$$

- Vertical:

$$\begin{aligned} \operatorname{ord} \operatorname{loc}_{q_1} c_M(n,Q) &= \operatorname{ord} \operatorname{loc}_{q_2} c_M(n, Qq_1q_2) \\ &= \operatorname{ord} \ell_M(n, Qq_1) \end{aligned}$$

Proof strategy

- Produce a single $Q = q_1 \cdots q_t$ such that

$$\ell_M(1, Q) \neq 0,$$

  and $q_1 \cdots q_i$ are all level-raising sets.

- By vertical relation:

$$\ell_M(n, q_1 \cdots q_i) \neq 0 \implies c_M(n, q_1 \cdots q_{i-1}) \neq 0$$

- By horizontal and vertical relation:

$$c_M(n, q_1 \cdots q_i) \neq 0 \implies \ell_M(n', q_1 \cdots q_{i-1}) \neq 0,$$

  where n' may have one additional prime factor.

- So for some n, $c_M(n, 1) \neq 0$ or $\ell_M(n, 1) \neq 0$.

Proof strategy

- Produce a single $Q = q_1 \cdots q_t$ such that

$$\ell_M(1, Q) \neq 0,$$

  and $q_1 \cdots q_i$ are all level-raising sets.
- By vertical relation:

$$\ell_M(n, q_1 \cdots q_i) \neq 0 \implies c_M(n, q_1 \cdots q_{i-1}) \neq 0$$

- By horizontal and vertical relation:

$$c_M(n, q_1 \cdots q_i) \neq 0 \implies \ell_M(n', q_1 \cdots q_{i-1}) \neq 0,$$

  where n' may have one additional prime factor.
- So for some n, $c_M(n, 1) \neq 0$ or $\ell_M(n, 1) \neq 0$.

The role of lifting

Suppose the level-raising map $\mathbb{Z}[X_{N^+,N^-Q}]^0 \twoheadrightarrow \mathbb{Z}/p^M(f)$ lifts to a Hecke eigenfunction ϕ_g. Then:

$$\ell_M(1,Q) \equiv L^{alg}(g/K,1) \pmod{p^M}$$

By work of Skinner-Urban, Wan, Kato, Ribet-Takahashi, Pollack-Weston, ...

$$v_{\mathfrak{p}} L^{alg}(g/K,1) =^* \lg_{\mathcal{O}_{\mathfrak{p}}} \mathrm{Sel}(K, A_g[\mathfrak{p}^\infty]) + \sum_{\ell | N^+} v_{\mathfrak{p}} t_g(\ell)$$

The role of lifting

Suppose the level-raising map $\mathbb{Z}[X_{N^+,N^-Q}]^0 \twoheadrightarrow \mathbb{Z}/p^M(f)$ lifts to a Hecke eigenfunction ϕ_g. Then:

$$\ell_M(1, Q) \equiv L^{alg}(g/K, 1) \pmod{p^M}$$

By work of Skinner-Urban, Wan, Kato, Ribet-Takahashi, Pollack-Weston, ...

$$v_{\mathfrak{p}} L^{alg}(g/K, 1) =^{*} \lg_{\mathcal{O}_{\mathfrak{p}}} \operatorname{Sel}(K, A_g[\mathfrak{p}^\infty]) + \sum_{\ell | N^+} v_{\mathfrak{p}} t_g(\ell)$$

By choosing M large and Q wisely, the right hand side can be made $< M$.

Deformation theory

- We want to choose a level-raising set Q such that there exists g of level NQ, congruent to f modulo p^M.
- By modularity lifting, suffices to find

$$\tau_g : G_{\mathbb{Q},S\cup Q} \to GL_2(\mathbb{Z}_p)$$

with appropriate local behavior and

$$\tau_g \equiv \rho_E \pmod{p^M}.$$

- Also want $v_{\mathfrak{p}} L^{alg}(g/K,1)$ to be small, i.e., $\mathrm{Sel}_Q(K,E[p^M])$ to be small.

Deformation theory (Ramakrishna, Fakhruddin-Khare-Patrikis)

Suffices to find k and Q s.t.:

- the image of

$$\mathrm{Sel}_{S\cup Q}(\mathbb{Q}, \mathrm{ad}^0 E[p^k]) \to \mathrm{Sel}_{S\cup Q}(\mathbb{Q}, \mathrm{ad}^0 E[p])$$

  is trivial (gives τ, then $g \equiv f \pmod{p^M}$)

Deformation theory (Ramakrishna, Fakhruddin-Khare-Patrikis)

Suffices to find k and Q s.t.:

- the image of

$$\mathrm{Sel}_{S\cup Q}(\mathbb{Q}, \mathrm{ad}^0 E[p^k]) \to \mathrm{Sel}_{S\cup Q}(\mathbb{Q}, \mathrm{ad}^0 E[p])$$

  is trivial (gives τ, then $g \equiv f \pmod{p^M}$)

- $\nu(N^- Q)$ is odd
- A_g will have small Selmer group, i.e. $\mathrm{Sel}_Q(K, E[p^M])$ is small

Then $v_{\mathfrak{p}} L^{alg}(g/K, 1)$ is small, so

$$\ell_M(1, Q) \neq 0$$